**Ransomware Attack on Primary-Care Health Clinic**

|  |  |
| --- | --- |
| **Date:** June 6, 2024 | **Entry:** 1 |
| **Description** | Documenting a cybersecurity incident |
| **Tool(s) used** | None |
| **The 5 W's** | * **Who:** An organized group of unethical hackers who are known to target organizations in healthcare and transportation industries * **What:** A ransomware attack * **Where:** At a small U.S. health care clinic specializing in primary-care services * **When:** Tuesday at 9:00 a.m. * **Why:** The incident occurred due to the unethical hackers group successfully executing a phishing attack, which granted them access to the clinic's systems. After getting access, they deployed ransomware that encrypted essential files. The primary motivation appears to be financial, as indicated by the ransom note demanding a significant sum for the decryption key. |
| **Additional notes** | 1. How could the health care organization prevent an incident like this in the future? 2. Is it advisable for the company to pay the ransom to obtain the decryption key? |